



WordPress LadiApp plugin <= 4.4 - Broken Access Control lead to XSS vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2023-49158
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-12-09 13:15:34 UTC
Updated	2026-04-29 10:16:27 UTC
Description	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Binh Nguyen LadiApp I

Risk And Classification

Primary CVSS: v3.1 7.1 HIGH from audit@patchstack.com

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L

EPSS: 0.002950000 probability, percentile 0.526770000 (date 2026-05-05)

Problem Types: CWE-79 | CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L
3.1	CNA	CVSS	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Binh Nguyen	LadiApp	affected 4.4 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/ladipage/vulnerability/wordpress-la...	audit@patchstack.com	patchstack.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, and

Vendor Comments And Credit

Discovery Credit

CNA: Truoc Phan | Patchstack Bug Bounty Program (en)

There are currently no legacy QID mappings associated with this CVE.